Math 357
Exam 03

2024–04–30 (T)

Your name: ______________________________

Honor pledge:

Instructions

1. In the space above, please legibly write your name and the Rice Honor Pledge, then sign.
2. Full time for this exam is exactly three hours. No resources are allowed.
3. Your reasoning—correctness and clarity—is more important than your "answer".
4. If you think there is ambiguity or error in an exercise, then briefly (!) write your understanding of the exercise and any additional hypotheses you are making, then proceed.

This exam is an imperfect measure of my understanding at a particular point in time. It is not a measure of who I am or who I will be.

Exercise	Total	(a)	(b)	(c)	(d)
Part 1					
1	/4	/4	/4	/4	/4
2	/4	/4	/4	/4	/4
3	/4	/4	/4	/4	
4	/4	/4	/4	/4	/4
Total	/16				
Part 2					
5	/4	/4	/4	/4	
6	/4	/4	/4	/4	/4
7	/4	/4	/4	/4	/4
8	/4	/4	/4	/4	/4
Total	/16				

Exercise 1

Let R be a commutative ring with a multiplicative identity $1_R \neq 0_R$, and let $I \subseteq R$.

(a) Define what it means for I to be (i) an ideal, (ii) a prime ideal, and (iii) a maximal ideal.

(b) Let I be an ideal of R. Prove that if I is maximal, then I is prime. (*Hint:* Use quotient rings.)

(c) Give an example to show that the converse to the statement in part (b) is false, in general. That is, give an example of a prime ideal that is not maximal.

(d) For each $i \in \mathbf{Z}_{>0}$, let I_i be an ideal of R such that $I_1 \subseteq I_2 \subseteq \ldots$. Prove that $I = \cup_{i \in \mathbf{Z}_{>0}} I_i$ is an ideal of R.

Exercise 2

(a) Define (i) integral domain, (ii) principal ideal domain, and (iii) field.

(b) Clearly present the logical implications among the following seven algebraic structures (no proof required):

> abelian group, euclidean domain (ED), field, integral domain (ID), principal ideal domain (PID), ring, unique factorization domain (UFD)

(c) Let R be a PID, and let $I \subseteq R$ be a prime ideal such that $I \neq (0_R)$. Prove that I is maximal.

(d) Now let R be a commutative ring, and let t be an indeterminate. Prove that the polynomial ring $R[t]$ is a PID if and only if R is a field.

Exercise 3

Let t be an indeterminate. We may give $\mathbf{Q}[t]$ the structure of a ring, a $\mathbf{Q}[t]$-module, or a $\mathbf{Z}$-module. For each map below, state whether it is a ring homomorphism, a $\mathbf{Q}[t]$-module homomorphism, or a $\mathbf{Z}$-module homomorphism. Justify your assertions. *Hint:* A given map may satisfy several or none of these conditions.

$$\begin{aligned} \varphi_1 : \mathbf{Q}[t] &\to \mathbf{Q}[t] \\ f(t) &\mapsto 0 \end{aligned} \qquad \begin{aligned} \varphi_2 : \mathbf{Q}[t] &\to \mathbf{Q}[t] \\ f(t) &\mapsto 2f(t) \end{aligned} \qquad \begin{aligned} \varphi_3 : \mathbf{Q}[t] &\to \mathbf{Q}[t] \\ f(t) &\mapsto f(t^2) \end{aligned}$$

Exercise 4

(a) Let $D_8 = \langle r, s \mid r^4, s^2, (rs)^2 \rangle$ be a presentation of the dihedral group of order 8. For each map below, state whether it defines a valid matrix representation of D_8. Justify briefly.

$$\begin{aligned} \rho_1 : D_8 &\to M_2(\mathbf{Q}) \\ r &\mapsto \begin{bmatrix} 1 & \\ & 1 \end{bmatrix} \\ s &\mapsto \begin{bmatrix} 1 & \\ & 1 \end{bmatrix} \end{aligned} \qquad\qquad \begin{aligned} \rho_2 : D_8 &\to M_2(\mathbf{Q}) \\ r &\mapsto \begin{bmatrix} & 1 \\ -1 & \end{bmatrix} \\ s &\mapsto \begin{bmatrix} & 1 \\ 1 & \end{bmatrix} \end{aligned}$$

Now let G be a finite group, let K be a field, and let V be a K-vector space.

(b) Let $\rho : G \to GL(V)$ be a representation of G on V. Explain the induced KG-module structure on V. In particular, specify $(\sum_{g \in G} \alpha_g g) \cdot v$, the ring action of the group ring KG on V.

(c) Define what it means for a module to be (i) decomposable, (ii) reducible, and (iii) completely reducible. (Recall that a representation has one of these properties if the KG-module that affords the representation has that property.)

(d) Further suppose that $\operatorname{char} K \nmid \#G$. Let ρ be a matrix representation of G of degree 2; and let $g_1, g_2 \in G$ such that $\rho(g_1)$ and $\rho(g_2)$ do not commute. Prove that ρ is irreducible.

Exercise 5

Let $K : K_0$ be a field extension, let $f \in K_0[t]$, and let $\alpha \in K$.

(a) Briefly explain the difference between viewing f as a polynomial and viewing f as a function. Give two distinct polynomials that define the same function. Justify briefly.

(b) Prove that $f(\alpha) = 0_K$ if and only if $t - \alpha$ divides f in $K[t]$.

(c) Further suppose that $[K : K_0] < \infty$, that f is irreducible in $K_0[t]$, and that $\gcd(\deg f, [K : K_0]) = 1$. Prove that f is irreducible in $K[t]$.

Exercise 6

Let K_0 be a field, let t be an indeterminate, and let $f \in K_0[t]$.

(a) Define what it means for f to be (i) irreducible and (ii) separable. Which of these definitions depends on the polynomial ring in which we consider f? Justify briefly.

Now let $f = t^4 - 4t^2 - 5 \in \mathbf{Q}[t]$.

(b) Show that f is separable and reducible in $\mathbf{Q}[t]$.

(c) Prove that $\mathbf{Q}(\sqrt{-1}, \sqrt{5}) \subseteq \mathbf{C}$ is a splitting field for f over $\mathbf{Q}$.

(d) Prove that $1, \sqrt{5}, \sqrt{-1}, \sqrt{-5}$ is a basis for $\mathbf{Q}(\sqrt{-1}, \sqrt{5})$ as a $\mathbf{Q}$-vector space. Use this basis to specify $\mathrm{Aut}(\mathbf{Q}(\sqrt{-1}, \sqrt{5}) : \mathbf{Q})$. In particular, show that $\mathrm{Aut}(\mathbf{Q}(\sqrt{-1}, \sqrt{5}) : \mathbf{Q})$ is generated by two automorphisms, and specify the relations that they satisfy.

Exercise 7

We continue to consider the polynomial $f = t^4 - 4t^2 - 5 \in \mathbf{Q}[t]$ from Exercise 6.

(a) Give two distinct arguments that the field extension $\mathbf{Q}(\sqrt{-1}, \sqrt{5}) : \mathbf{Q}$ is galois.

(b) Draw a diagram of subgroups of $\mathrm{Aut}(\mathbf{Q}(\sqrt{-1}, \sqrt{5}) : \mathbf{Q})$ and a diagram of subfields (intermediate fields) of $\mathbf{Q}(\sqrt{-1}, \sqrt{5}) : \mathbf{Q}$. Clearly indicate the galois correspondences.

(c) Let $\alpha = \sqrt{-1} + \sqrt{5} \in \mathbf{C}$. Prove that $\mathbf{Q}(\alpha) = \mathbf{Q}(\sqrt{-1}, \sqrt{5})$. *Hint:* Consider α^{-1}.

(d) Find the minimal polynomial $m_{\alpha,\mathbf{Q}}$ of α over $\mathbf{Q}$. Justify that it satisfies all defining axioms of a minimal polynomial.

Exercise 8

This exercise, combined with the theory of solvable groups, shows that the general quintic (and hence the general polynomial of degree $n \geqslant 5$) cannot be solved by radicals.

Let $f = t^5 - 6t + 3 \in \mathbf{Q}[t]$, and let $K_f \subseteq \mathbf{C}$ be the splitting field for f in $\mathbf{C}$.

(a) Prove that f is irreducible in $\mathbf{Q}[t]$. Deduce that $5 \mid [K_f : \mathbf{Q}]$.

(b) Prove that f has exactly three zeros in $\mathbf{R}$ and exactly two zeros in $\mathbf{C} - \mathbf{R}$. You may use the values in the table below in your proof.

t	-2	-1	0	1	2
$f(t)$	-17	8	3	-2	23
$f'(t)$	74	-1	-6	-1	74

(c) Let $\tau_{\mathbf{C}} : \mathbf{C} \to \mathbf{C}$ denote the automorphism of $\mathbf{C}$ of complex conjugation (that is, for all $a, b \in \mathbf{R}$, $\tau_{\mathbf{C}}(a + bi) = a - bi$), and let $\tau \in \mathrm{Aut}(K_f : \mathbf{Q})$ be the restriction of $\tau_{\mathbf{C}}$ to K_f. Prove that τ fixes the three real zeros of f and swaps the two non-real complex ones.

(d) Justify why $K_f : \mathbf{Q}$ is galois. Deduce that $\mathrm{Gal}(K_f : \mathbf{Q}) \cong S_5$, the symmetric group on five elements. *Hint:* You may use without proof the fact that S_5 is generated by $\{\sigma_2, \sigma_5\}$, where $\sigma_m \in S_5$ is an m-cycle.